QD-IM-005
REVISION D
Effective Date: September 24, 2004

ORGANIZATIONAL INSTRUCTION

SERVER MANAGEMENT FOR SAFETY & MISSION ASSURANCE

OPR(s)	**OPR DESIGNEE**
QD03, QD40	**Teresa Durrette**

DOCUMENT HISTORY LOG

Status (Baseline/ Revision/ Canceled)	Document Revision	Effective Date	Description
Baseline		2/16/00	
Revision	A	9/04/02	Format and numbering change to implement requirements of QS-A-001 rev F. The numbering scheme changed on this document from QS10-MI-005 to QS-IM-005. The "MI" changed to "IM".
Revision	B	6/16/03	Deleted references to OIs. Added/revised Applicable and Reference documents. Incorporated revisions to section 4.0 Instructions driven by revisions to NPG 2810.1. Incorporated miscellaneous wording changes for clarification. Changed references from OCIO to IT Manager. Updated Quality Records requirements due to process changes within MSFC that changed record owner.
Revision	C	03/05/04	Revised to reflect process changes due to shared ownership of administration duties with the center's IT contractor and to incorporate minor edits.
Revision	D	9/24/04	Revised to bring document in compliance with the HQ Rules Review Action (CAITS: 04-DA01-0387). Changes were also made to reflect S&MA organizational name changes (i.e., QS to QD). Format changes

SERVER MANAGEMENT FOR SAFETY AND MISSION ASSURANCE

1. PURPOSE, SCOPE, APPLICABILITY (As Required)

1.1 Purpose – These instructions establish the procedures for S&MA server management to ensure data integrity and compliance to upper level procedures.

1.2. Scope – This Organizational Issuance (OI) provides instructions for managing server as an Information Technology resource for S&MA.

1.3. Applicability – The processes described herein apply to any IT resource that is 1) operating as a server for the S&MA organization; and 2) administered by S&MA personnel or delegate.

2. DOCUMENTS (Applicable and/or Reference)

2.1. Applicable Documents –

MPD 2800.1 – "Management of Information Technology Systems & Services at MSFC"
MPD 2810.1 - "Security of Information Technology"
MPR 2810.1 – "Security of Information technology"

2.2. Reference Documents

MSFCSMA5 Security Plan
QD Web Products Application Security Plan
MSFC Problem Reporting and Corrective Action System Application Security Plan

3. DEFINITIONS

3.1 Server Administration – The management of a multi-user computer system. Management includes any and all of the following functions: assurance of licensing adequacy, software upgrades, version control, backup and recovery, operating system control, printer spooling, job scheduling, security assurance, virus protection and performance and capacity planning.

3.2 Server Administrator – The S&MA individual charged with assurance of server administration duties for a particular server. May also be called "administrator".

3.3 Server - A computer and its components that provides a specific kind of service or services, such as file storage or application hosting and web promoting. In this instance, server only refers to the software, middleware, freeware, applications, files and processes that work together to perform a function and is designated by the server name.

3.4 Server Notebook - A collection of notes made by the server administrator documenting the server's hardware and software configuration. The server configuration must be maintained current, and the notebook will be stored in the server administrator's normal working location.

3.5 Information Technology (IT) – Includes all electronic processing equipment as well as software items and products.

3.6 Organizational Computer Security Official (OCSO) – S&MA employee assigned by the Director who is responsible for IT security within the Directorate.

3.7 IT Manager - S&MA employee assigned by the Director who coordinates IT issues within the Directorate and coordinates issues with the center's office of the Chief Information Official. Duties of the IT Manager may be delegated.

4. INSTRUCTIONS

4.1 The IT Manager shall assure that a server administrator is designated by the appropriate line manager for each server operated by S&MA. The server administrator is responsible for:

4.1.A Implementing procedures to meet all requirements contained herein for the server(s) under his/her control.

4.1.B Operating each server according to requirements established by the responsible line manager.

4.1.C Assuring that supporting processes are in place and are being met routinely.

4.1.D Assuring that a database of system administrators; owner organizations and Points of Contact; line manager; applicable security plan; date of last risk assessment; status of required training; and date of authorization to process is maintained.

4.1.E Coordinating procurement needs identified by the administrator for approval and processing.

4.2 Server Administration - The server administrator is responsible for administration activities (see flow chart in section 11.1) including:

4.2.1 Hardware/Software Installation and Configuration – The server administrator shall:

4.2.1.A Install and configure server software with assistance provided by manufacturers as necessary.

4.2.1.B Document installation and configuration procedures and changes in the server

notebook. For previously established servers, the administrator shall perform a software assessment and document the configuration of the server in the server notebook at the time of assessment.

4.2.1.C Monitor server performance per paragraph 4.2.4 and recommend changes affecting requirements to the line manager and the IT Manager.

4.2.2 Operating System, Database and Other Software Maintenance – The administrator shall:

4.2.2.A Upgrading the Operating System as applicable, database product and other software, middleware or freeware products that are resident on the server and for applying any necessary patches or fixes.

4.2.2.B Evaluate the benefits and risks of incorporating upgrades or fixes and document the configuration change in the server notebook.

4.2.2.C Perform upgrades during low server demand hours unless the line manager approves the upgrade during heavy usage hours.

4.2.2.D Notified users in advance of potential server downtime as possible.

4.2.3 Application Integration and Hosting – The administrator shall:

4.2.3.A Assist users by installing applications upon approval by the Curator.

4.2.3.B Perform all activities required during the installation process, including 1) creation of directories; 2) assignment of user privileges and rights; 3) creation of an ODBC data source; and 4) modification of menus.

4.2.3.C Assure that unused, inactive or unnecessary software applications and associated files and directories are removed or disabled.

4.2.3.D Review servers annually at a minimum to identify inactive or unnecessary applications after approving their removal by the Curator.

4.2.4 Performance Monitoring – The administrator shall:

4.2.4.A Monitor server performance to identify potential problem areas.

4.2.4.B Analyze adverse trends and suggest improvements to the Line Manager.

4.2.5 Customer Support and Problem Resolution – The server administrator shall support users in resolving problems and providing necessary functionality. When problems are identified the

administrator shall research the problem and implement any necessary resolution. Feedback regarding problem resolution shall be provided to the user, IT Manager or help desk as necessary.

4.2.6 Hardware/Software Licensing and Maintenance Assurance – The administrator shall:

4.2.6.A Assure that information regarding software licensing is current and that information required to make support calls is maintained in the server notebook.

4.2.6.B Ensure licensing adequacy and identify associated procurement needs to the IT Manager for approval.

4.2.7 Storage Management – The server administrator shall:

4.2.7.A Perform routine backups as required by the security plan.

4.2.7.B Document in the server notebook procedures for required backups in the server notebook,

4.2.7.C Document changes in backup procedures in the server notebook and in the security plan during the yearly review.

4.2.8 Configuration Management and Documentation – The server administrator shall document the server software configuration and subsequent changes in the server notebook.

4.2.9 Account Creation and Assignment of Permissions – The server administrator shall create accounts, assign permissions, delete accounts and make changes to permissions as directed by the OCSO.

4.3 Server Security – The server administrator shall assure that all requirements of MPR 2810.1 “Security of Information Technology” are met and maintain security plans and server notebooks in secure files.

4.3.1 To maintain server certification, the server administrator shall:

4.3.1.A Maintain associated security plans current and assure that the plans have received Authorization to Process.

4.3.1.B Review each security plan at least yearly and revised as required by MPR 2810.1.

4.3.1.C Obtain approval from the OCSO and the Line Manager for changes in the security structure prior to implementation.

4.3.1.D Perform security-related activities required by MPR 2810.1, including performance of risk analysis, risk mitigation and processes supporting certification as described in section 4.4.2 of this document.

4.3.2 When a scan is performed on the server, the administrator shall:

4.3.2.A Review the results of scans performed;

4.3.2.B Assess the actions necessary to resolve each problem;

4.3.2.C Determine the impact of implementing the resolution;

4.3.2.D Resolve the problem or determine not to implement the resolution;

4.3.2.E Document on the scan results the date of implementation or the rationale for not implementing;

4.3.2.F Report the results per requirements of MPR 2810.1

4.3.2.G Maintain scan result records in the security files, which are located in the administrator's normal work area in a secure environment.

4.3.2.H Document server changes in the server notebook. (See flow diagram in section 11.2.)

4.3.3. The administrator shall assure that server logs are maintained for each software server per requirements of MPR 2810.1 and shall:

4.3.3.A Review logs weekly at a minimum to identify unauthorized activity.

4.3.3.B Report suspected unauthorized activity to the OCSO.

4.3.3.C Participate in investigations.

4.3.3.D Purge logs monthly at a minimum.

4.3.3.E Maintain evidence of unauthorized activity in the security file as long as required by the OCSO and by the Center IT Security group (See flow diagram in section 11.3.)

4.4 To prepare for disaster recovery, the administrator shall:

4.4.A Maintain server notebooks for use in recreating server configuration.

4.4.B Use data backups for recovery of data and server reconfiguration in the event of

catastrophic loss.

4.4.C Assure that servers housed at the administrator's work location have a properly configured UPS attached and software installed to shut down server processes in the event of a power interruption as required by the Line Manager.

4.4.D Implement special provisions for disaster recovery, such as standby hardware/software systems or hot-swappable disks, as required by the risk analysis and included in the security plan.

5. NOTES (References)

5.1. OI Replacement - This instruction replaces QS-IM-005 Revision C, "Server Management for Safety and Mission Assurance", dated 03/06/2004

6. SAFETY PRECAUTIONS AND WARNING NOTES
Not Applicable

7. APPENDICES, DATA, REPORTS, AND FORMS
Not Applicable

8. RECORDS

Record	Repository	Period of Time
Server Administrator Database	QD03: IT MANAGER OR DELEGATE-designated record custodian; Maintained Electronically (and encrypted) in ITS_QD.xls file stored in the INFORMAT.MGT\IT Manager folder of S&MA's shared file storage area	NPG1441.1 Records Retention Schedules. Schedule 2400/13D2 DELETE AFTER THE EXPIRATION OF THE RETENTION PERIOD AUTHORIZED FOR THE HARD COPY. IF THE ELECTRONIC VERSION REPLACES HARD COPY RECORDS WITH DIFFERING RETENTION PERIODS, AND AGENCY SOFTWARE DOES NOT READILY PERMIT SELECTIVE DELETION, DELETE AFTER THE LONGEST RETENTION PERIOD HAS EXPIRED. [GRS 20-15b]
Server Notebook	QD03- Assigned Server Administrator. Maintained Electronically or by hard copy in server	NPG1441.1 Records Retention Schedules. Schedule 2410/14D3 Retain with related data files. Destroy in accordance with related files.

	administrator's work area	
Backup Media	QD03-Assigned Server Administrator. Electronic storage media. Managed per security plan.	NPG1441.1 Records Retention Schedules. Schedule 2420/15C1 Release media for reuse after preparation of third generation. Release no earlier than 6 months after generation of preceding interim media. [GRS 20] (N 27-4)
Scan Results/Log Files/Evidence of Unauthorized activity	QD03: IT MANAGER-designated record custodian; Maintained electronically or in hard copy in a secure location in the Administrator's work area	NPG1441.1 Records Retention Schedules. Schedule 2420/15A3 Delete/Destroy when no longer needed for administrative, legal, audit or other operational purposes.
Security Plan	QD03: OCSO record retained by System Administrator; hard copy maintained in access-restricted system files in Administrator's work area.	2410/14.b.2 Destroy when active reference value ceases or when 3 years old, whichever is later.

9. TOOLS, EQUIPMENT, AND MATERIALS

None

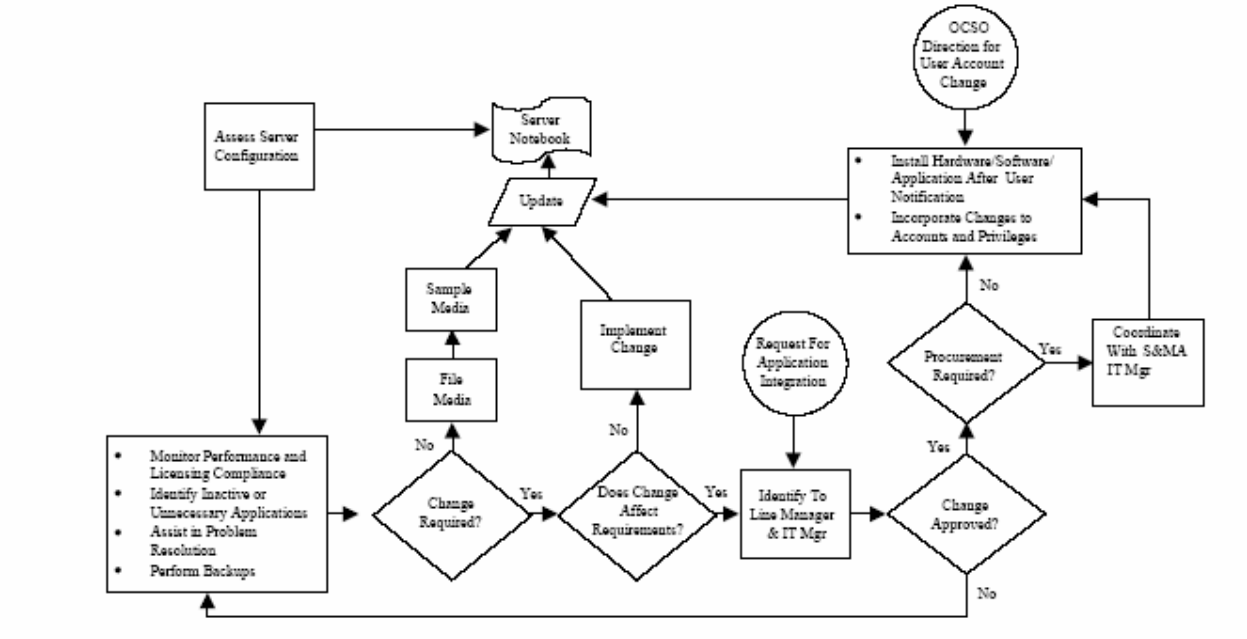
10. PERSONNEL TRAINING AND CERTIFICATION

10.1 PERSONNEL TRAINING AND CERTIFICATION

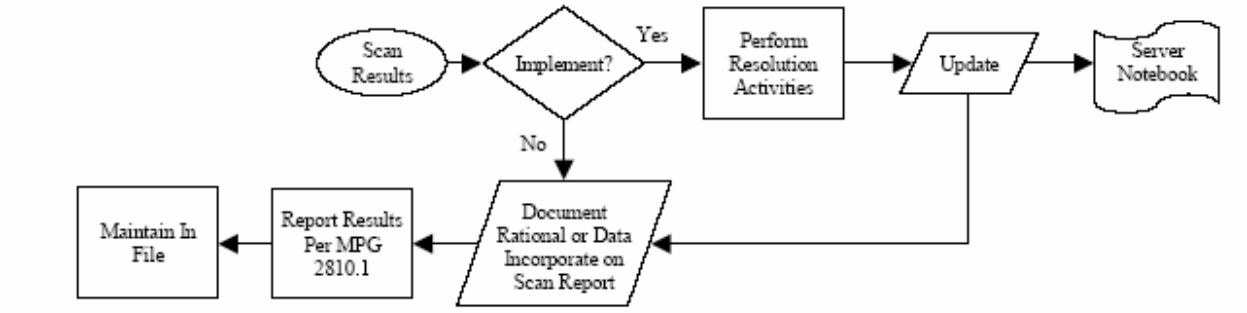
Administrators shall possess a minimum of two years' experience as a server administrator and a minimum 1 year experience with the applicable operation system. Backup Administrators shall possess a minimum 1 year experience with server administration duties. Administrators and Backup Administrators shall assure that documentation regarding completion of required certification per MPR 2810.1 is entered into his/her Official Personnel Record.

11. FLOW DIAGRAM

11.1 Server Administration



11.2 Server Scans



11.3 Server Logs